PTO/SB/21 (08-03)
Approved for use through 08/30/2003. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Application Number	10/692,493
Filing Date	10/24/03
First Named Inventor	Yuji Suga
Art Unit	2124
Examiner Name	
Attorney Docket Number	CFA00034US

Total Number of Pages in This Submission: 52

ENCLOSURES *(Check all that apply)*

- ☐ Fee Transmittal Form
  - ☐ Fee Attached
- ☐ Amendment/Reply
  - ☐ After Final
  - ☐ Affidavits/declaration(s)
- ☐ Extension of Time Request
- ☐ Express Abandonment Request
- ☐ Information Disclosure Statement
- ☑ Certified Copy of Priority Document(s)
- ☐ Response to Missing Parts/ Incomplete Application
  - ☐ Response to Missing Parts under 37 CFR 1.52 or 1.53
- ☐ Drawing(s)
- ☐ Licensing-related Papers
- ☐ Petition
- ☐ Petition to Convert to a Provisional Application
- ☐ Power of Attorney, Revocation Change of Correspondence Address
- ☐ Terminal Disclaimer
- ☐ Request for Refund
- ☐ CD, Number of CD(s) _____
- ☐ After Allowance communication to Technology Center (TC)
- ☐ Appeal Communication to Board of Appeals and Interferences
- ☐ Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- ☐ Proprietary Information
- ☐ Status Letter
- ☐ Other Enclosure(s) (please Identify below):

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm or Individual name	Canon U.S.A., Inc. IP Department Fidel Nwamu
Signature	Fidel Nwamu
Date	2/11/04

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below.

Typed or printed name	Fidel Nwamu		
Signature	Fidel Nwamu	Date	2 11 04

CFA 00034
US

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００２年１０月２９日

出願番号
Application Number: 特願２００２－３１４５９５

[ST. 10/C]: [ＪＰ２００２－３１４５９５]

出願人
Applicant(s): キヤノン株式会社

２００３年１１月１８日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号 出証特２００３－３０９４９９６

【書類名】　特許願
【整理番号】　4823011
【提出日】　平成14年10月29日
【あて先】　特許庁長官　太田　信一郎　殿
【国際特許分類】　G06F 17/00
【発明の名称】　べき乗演算装置
【請求項の数】　1
【発明者】
【住所又は居所】　東京都大田区下丸子３丁目３０番２号キヤノン株式会社内
【氏名】　須賀　祐治
【特許出願人】
【識別番号】　000001007
【住所又は居所】　東京都大田区下丸子３丁目３０番２号
【氏名又は名称】　キヤノン株式会社
【代表者】　御手洗　冨士夫
【電話番号】　03-3758-2111
【代理人】
【識別番号】　100090538
【住所又は居所】　東京都大田区下丸子３丁目３０番２号キヤノン株式会社内
【弁理士】
【氏名又は名称】　西山　恵三
【電話番号】　03-3758-2111

【選任した代理人】

【識別番号】　100096965

【住所又は居所】　東京都大田区下丸子３丁目３０番２号キヤノン株式会社内

【弁理士】

【氏名又は名称】　内尾　裕一

【電話番号】　03-3758-2111

【手数料の表示】

【予納台帳番号】　011224

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9908388

【プルーフの要否】　要

【書類名】　　明細書

【発明の名称】　べき乗演算装置

【特許請求の範囲】

【請求項１】　２つの整数ｘおよびｅからｘｅを計算するべき乗演算装置において、

２つの整数ｘおよびｅを入力する入力手段と、

Ｌ個の候補指数｛ｌ＿ｉ｝（０≦ｉ≦Ｌ－１）を格納する候補指数格納手段と、

前記候補指数格納手段に格納されている候補指数｛ｌ＿ｉ｝のそれぞれに対し、入力された整数ｘからｘ＾｛ｌ＿ｉ｝を事前に計算しておく事前計算手段と、

事前計算された数値ｘ＾｛ｌ＿ｉ｝を格納する事前計算数値格納手段と、

入力された整数ｅを前記候補指数｛ｌ＿ｉ｝のいずれかと一致するように複数の数値｛ｆ＿ｉ｝（０≦ｉ≦Ｆ－１）に分割する分割手段と、

計算結果ｃを格納する計算結果格納手段と、

分割された数値｛ｆ＿ｉ｝（０≦ｉ≦Ｆ－１）について、事前計算された数値ｘ＾｛ｌ＿ｉ｝を用いて計算結果ｃを逐次更新する逐次処理手段と、

全ての前記数値｛ｆ＿ｉ｝について更新後の計算結果ｃをｘｅとして出力する出力手段と

を有することを特徴とするべき乗演算装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、べき乗剰余演算などにおけるべき乗演算を行なう、べき乗演算装置に関するものである。

【０００２】

【従来の技術】

べき乗剰余演算ｘｅ（ｍｏｄ　Ｎ）は、ＲＳＡ暗号／署名をはじめＥｌＧａｍａｌ暗号、ＤＳＡ署名、Ｄｉｆｆｉｅ-Ｈｅｌｌｍａｎ鍵共有方式などで利用されている演算である。ファイルに対する署名や復号などの用途だけではなくＳＳ

Ｌなどの通信路のセキュア化においても利用されており、通信要求に対してインタラクティブに演算を行う必要があり、処理効率は暗号処理計算時間に大きく影響する。

【０００３】

べき乗剰余演算はａ）平方剰余演算x^2（ｍｏｄ　Ｎ）と、ｂ）乗算剰余演算ｘｕ（ｍｏｄ　Ｎ）とにより構成することができる。与えられたｅに対しｘｅ（ｍｏｄ　Ｎ）を計算するために必要とするａ）およびｂ）の乗算演算の回数を削減することにより、全体の処理時間を高速化する手法がいくつか提案されている。

【０００４】

加算鎖（ａｄｄｉｔｉｏｎ　ｃｈａｉｎ）とは、$a_1=1$からはじまり最終的に$a_n=e$に至る整数の列であり、a_iはそれ以前に現れた数の和（つまり$a_i=a_j+a_k$（ｊ，ｋ＜ｉ））を満たす。例えばｅ＝５５のとき｛１，２，３，６，１２，１３，２６，２７，５４，５５｝はその例である。これは$x\rightarrow x^2\rightarrow x^3\rightarrow x^6\rightarrow x^{12}\rightarrow x^{13}\rightarrow x^{26}\rightarrow x^{27}\rightarrow x^{54}\rightarrow x^{55}$のようにａ）およびｂ）の演算を行うことで、$x^{55}$が計算できることを表している。これは｛１，２，３，４，…，５２，５３，５４，５５｝のようにｂ）の演算だけを用いるよりも計算量を少なくすることができることを意味している。このように、与えられた指数ｅ（上の例では５５）に対し、より短い加算鎖を見つけるアルゴリズムが有益である。

【０００５】

〔Ｂｉｎａｒｙ　Ｍｅｔｈｏｄ〕

Ｂｉｎａｒｙ　Ｍｅｔｈｏｄは上記のモチベーションに基づいたアルゴリズムの一つであり、Ｄ．Ｅ．Ｋｎｕｔｈ．Ｔｈｅ　Ａｒｔ　ｏｆ　Ｃｏｍｐｕｔｅｒ　Ｐｒｏｇｒａｍｍｉｎｇ：Ｓｅｍｉｎｕｍｅｒｉｃａｌ　Ａｌｇｏｒｉｔｈｍｓ，ｖｏｌｕｍｅ　２，Ｒｅａｄｉｎｇ，ＭＡ：Ａｄｄｉｓｏｎ－Ｗｅｓｌｅｙ，Ｓｅｃｏｎｄ　ｅｄｉｔｉｏｎ（１９８１）で紹介されている。

【０００６】

Ｂｉｎａｒｙ　Ｍｅｔｈｏｄは、次のような処理を行うアルゴリズムである。

与えられた指数ｅ（ｋビット長）をΣｉ－０，…，ｋ－１２ｉ＊ｅ＿ｉ（ｅ＿ｉは０または１）のように２進表現しておく。入力をｘ，ｅ，Ｎとし、出力Ｃはｘｅ（ｍｏｄ　Ｎ）となるアルゴリズムは以下のとおりである。

【０００７】

１）ｉｆ　ｅ＿（ｋ－１）＝１ｔｈｅｎ　Ｃ：＝ｘ　ｅｌｓｅ　Ｃ：＝１

２）ｆｏｒ　ｉ＝ｋ－２　ｄｏｗｎｔｏ　０

２－１）Ｃ：＝Ｃ＊Ｃ（ｍｏｄ　Ｎ）

２－２）ｉｆ　ｅ＿ｉ＝１ｔｈｅｎ　Ｃ　：＝Ｃ　＊　ｘ　（ｍｏｄ　Ｎ）

３）ｒｅｔｕｒｎ　Ｃ

上記において、２）のｆｏｒは変数ｉがｋ－２から０まで１ずつ削減ながら２－１）及び２－２）をループ処理することを表している。図２はｅ＝５５のときＢｉｎａｒｙ　Ｍｅｔｈｏｄを使って上記のようにｘ５５（ｍｏｄ　Ｎ）が計算される過程を表したものである。このときの加算鎖は｛１，２，３，６，１２，１３，２６，２７，５４，５５｝である。

【０００８】

〔ｍ－ａｒｙ　Ｍｅｔｈｏｄ〕

ｍ－ａｒｙ　Ｍｅｔｈｏｄ　はＢｉｎａｒｙ　Ｍｅｔｈｏｄを拡張させたもので、２ビット以上の処理を一度に行う方式である。入力をｘ，ｅ，Ｎとし、出力Ｃはｘｅ（ｍｏｄ　Ｎ）となるアルゴリズムは以下の通りである。ただし、与えられた指数ｅはｋビット長であり、ｅはｓ個のｒ（＝ｌｏｇ２ｍ）ビット列Ｆ＿０，…，Ｆ＿（ｓ－１）（ただしｓはｋ／ｒを超えない整数）に分解されているとする。

【０００９】

０）ｗ＝２，…，ｍ－１についてｘｗ（ｍｏｄ　Ｎ）を事前に計算しておく

１）Ｃ：＝ｘ＾｛Ｆ＿（ｓ－１）｝（ｍｏｄ　Ｎ）とおく。

２）ｆｏｒ　ｉ＝ｓ－２　ｄｏｗｎｔｏ　０

２－１）Ｃ：＝Ｃｍ　（ｍｏｄ　Ｎ）

２－２）ｉｆ　Ｆ＿ｉ　≠０　ｔｈｅｎ　Ｃ：＝Ｃ　＊　ｘ＾｛Ｆ＿ｉ｝（ｍｏｄ　Ｎ）

３）ｒｅｔｕｒｎ　Ｃ

【００１０】

ｍ－ａｒｙ　Ｍｅｔｈｏｄ　は、ｍ＝４のときＱｕａｔｅｒｎａｒｙ　Ｍｅｔｈｏｄ　と呼ばれる。ｅ＝５５のときのＱｕａｔｅｒｎａｒｙ　Ｍｅｔｈｏｄの処理を図３に示す。Ｅを２進数表示すると（１１０１１１）$_2$であるが、これをｒ＝２ビットずつに分解すると、（１１　０１　１１）$_2$であり、図３に示されている通りに処理される。このときの加算鎖は｛1，２，３，６，１２，１３，２６，５２，５５｝であり、Ｂｉｎａｒｙ　Ｍｅｔｈｏｄに比べて加算鎖の長さが１つ短いため、ｘ５５を計算するための剰余演算が少なくて済むことを意味している。

【００１１】

さらにｍ－ａｒｙ　Ｍｅｔｈｏｄの拡張として、Ｓｌｉｄｅ　Ｗｉｎｄｏｗ　Ｔｅｃｈｎｉｑｕｅｓなど多くの改良案が提案されている。Ｓｌｉｄｅ　Ｗｉｎｄｏｗ　Ｔｅｃｈｎｉｑｕｅｓでは、固定長でなく、アルゴリズム中の２）の処理で１度に扱うビット長を可変長にすることで、アルゴリズム中の０）の処理にあたる事前計算処理を削減し、計算量の削減と事前計算結果を格納しておく領域（テーブルと呼ぶ）の削減を実現している。

【００１２】

【発明が解決しようとする課題】

上述した従来技術において、Ｂｉｎａｒｙ　Ｍｅｔｈｏｄは事前計算を行う必要がなく、事前計算結果を格納するテーブルを持つ必要がないというメリットを持つ。しかしｅを２進数表示したとき、１が立っているビットの個数が多い場合、計算処理を増大させてしまう欠点がある。また、Ｑｕａｔｅｒｎａｒｙ　Ｍｅｔｈｏｄ　やＳｌｉｄｅ　Ｗｉｎｄｏｗ　Ｔｅｃｈｎｉｑｕｅｓでは、計算量を少なくする利点があるが、テーブル参照が必要となり事前計算処理の計算量がかさむデメリットがある。

【００１３】

本発明は、ｅを２進数表示した際のビット列内にある特徴を持つビット列が登場することを想定し、それらのビット列に関してのみ事前計算を行うことで、事

前計算処理量とテーブルサイズを削減し、従来方式に比べて少ない演算回数で計算することができるべき乗計算方式を提供する。またテーブルサイズをおさえるメリットもあわせ持ち、テーブル参照のためのメモリ領域を削減することができる。

【００１４】

【課題を解決するための手段】

そこで、本発明の目的は、べき乗演算における事前計算処理量とテーブルサイズとを低減させ、少ない演算回数で計算することができるべき乗演算装置を提供することにある。

【００１５】

上記目的を達成するために、本発明では、２つの整数ｘおよびｅからｘｅを計算するべき乗演算装置に、２つの整数ｘおよびｅを入力する入力手段と、Ｌ個の候補指数｛ｌ＿ｉ｝（０≦ｉ≦Ｌ－１）を格納する候補指数格納手段と、前記候補指数格納手段に格納されている候補指数｛ｌ＿ｉ｝のそれぞれに対し、入力された整数ｘからｘ＾｛ｌ＿ｉ｝を事前に計算しておく事前計算手段と、事前計算された数値ｘ＾｛ｌ＿ｉ｝を格納する事前計算数値格納手段と、入力された整数ｅを前記候補指数｛ｌ＿ｉ｝のいずれかと一致するように複数の数値｛ｆ＿ｉ｝（０≦ｉ≦Ｆ－１）に分割する分割手段と、計算結果ｃを格納する計算結果格納手段と、分割された数値｛ｆ＿ｉ｝（０≦ｉ≦Ｆ－１）について、事前計算された数値ｘ＾｛ｌ＿ｉ｝を用いて計算結果ｃを逐次更新する逐次処理手段と、全ての前記数値｛ｆ＿ｉ｝について更新後の計算結果ｃをｘｅとして出力する出力手段とを備える。

【００１６】

【発明の実施の形態】

以下、図面を参照して、本発明の実施形態を説明する。

【００１７】

（第１の実施の形態）

本発明は、例えば、図１に示すような情報処理装置（ホストコンピュータ）１００に適用される。本実施形態の情報処理装置１００は、パーソナルコンピュー

タ等のコンピュータを含み、視覚復号型秘密分散法により、機密画像情報から複数の分散画像情報を生成して分配する機能を実現する。

【００１８】

すなわち、情報処理装置１００は、図１に示すように、公衆回線等のモデム１１８、表示部としてのモニタ１０２、ＣＰＵ１０３、ＲＯＭ１０４、ＲＡＭ１０５、ＨＤ１０６、ネットワークのネットワーク接続部１０７、ＣＤ１０８、ＦＤ１０９、ＤＶＤ１１０、プリンタ１１５のインターフェース（Ｉ／Ｆ）１１７、及び操作部としてのマウス１１２やキーボード１１３等のインターフェース（Ｉ／Ｆ）１１１が、バス１１６を介して互いに通信可能に接続された構成としている。

【００１９】

マウス１１２及びキーボード１１３は、ユーザが情報処理装置１００に対する各種指示等を入力するための操作部である。この入力情報（操作情報）は、インターフェース１１１を介して情報処理装置１００内に取り込まれる。

【００２０】

情報処理装置１００での各種情報（文字情報や画像情報等）は、プリンタ１１５により印刷出力できるようになされている。

【００２１】

モニタ１０２は、ユーザへの各種指示情報や、文字情報或いは画像情報等の各種情報の表示を行う。

【００２２】

ＣＰＵ１０３は、情報処理装置１００全体の動作制御を司る。すなわち、ＣＰＵ１０３は、ＨＤ（ハードディスク）１０６等から処理プログラム（ソフトウェアプログラム）を読み出して実行することで、情報処理装置１００全体を制御する。特に、本実施形態では、ＣＰＵ１０３は、機密画像情報から複数の分散画像情報を生成して分配するための処理プログラムを、ＨＤ１０６等から読み出して実行することで、後述する処理（以下、「情報分散処理」とも言う）を実施する。

【００２３】

ＲＯＭ１０４は、必要な画像処理のための処理プログラム、及び情報分散処理のための処理プログラム等の各種処理プログラムや、各種データ等を記憶する。

【００２４】

ＲＡＭ１０５は、ＣＰＵ１０３での各種処理のために一時的に処理プログラムや処理対象の情報を格納するための作業用エリア等として使用される。

【００２５】

ＨＤ１０６は、大容量記憶装置の一例としての構成要素であり、文字情報や画像情報、或いは各種処理の実行時にＲＡＭ１０５等へ転送される情報分散処理等のための処理プログラム等を保存する。

【００２６】

ＣＤ（ＣＤドライブ）１０８は、外部記憶媒体の一例としてのＣＤ（ＣＤ－Ｒ）に記憶されたデータを読み込み、また、当該ＣＤへデータを書き出す機能を有する。

【００２７】

ＦＤ（フロッピー（Ｒ）ディスクドライブ）１０９は、ＣＤ１０８と同様に、外部記憶媒体の一例としてのＦＤに記憶されたデータを読み込み、また、当該ＦＤへデータを書き出す機能を有する。

【００２８】

ＤＶＤ（ディジタルビデオディスクドライブ）１１０は、ＣＤ１０８やＦＤ１０９と同様に、外部記憶媒体の一例としてのＤＶＤに記憶されたデータを読み込み、また、当該ＤＶＤへデータを書き出す機能を有する。

【００２９】

尚、ＣＤ、ＦＤ、ＤＶＤ等の外部記憶媒体に対して、例えば、編集用のプログラム或いはプリンタドライバが記憶されている場合、これらをＨＤ１０６へインストールし、必要に応じてＲＡＭ１０５へ転送するように構成してもよい。

【００３０】

インターフェース（Ｉ／Ｆ）１１１は、マウス１１２やキーボード１１３によるユーザからの入力を受け付けるためのものである。

【００３１】

モデム１１８は、通信モデムであり、インターフェース（Ｉ／Ｆ）１１９を介して、例えば公衆回線等を通じて外部のネットワークに接続される。

【００３２】

ネットワーク接続部１０７は、インターフェース（Ｉ／Ｆ）１１４を介して外部のネットワークに接続される。

【００３３】

図４は、図1の情報処理装置１００において、特徴とする機能（情報分散処理の機能）に着目して図示したものである。情報処理装置１００は、図４に示すように、候補指数格納部４０２、事前計算モジュール４０３、事前計算数値格納部４０４、分割モジュール４０５、逐次処理モジュール４０６及び計算結果格納部４０７を有する。各モジュール４０３、４０５、４０７は、ＣＰＵ１０３が所定のプログラムを実行することで実現される機能単位（モジュール）を表わす。

【００３４】

情報処理装置１００に対しては、外部から入力値ｘ、Ｎ（４００）及びｅ（４０１）が入力される。情報処理装置１００は、入力値からべき乗剰余演算を行い結果として$c = x^e \pmod N$（４０８）を出力する装置である。入力値Ｎが入力されない場合には$c =$べき乗演算x^eを行うが、これはべき乗剰余演算の特殊な場合と考えられるため、第１の実施の形態では、べき乗剰余演算$x^e \pmod N$を行う装置の説明のみを行う。

【００３５】

候補指数格納部４０２には、あらかじめ、｛（１），（１０１），（１０１０１），…｝（２進数表示）のように$1\,[01]_L$（ただし$[xy]_i$はｉ回ｘｙを繰り返したもの）の形式を持つ数値が含まれている。事前計算モジュール４０３は、入力値（４００）と候補指数格納部４０２から事前計算を行い、事前計算結果を、例えばＨＤ１０６にある、事前計算数値格納部４０４に格納する。分割モジュール４０５は、入力値４０１を分割し、入力値４０１および分割された数値を、例えばＨＤ１０６に格納する。逐次処理モジュール４０６は、例えばＨＤ１０６にある計算結果格納部４０７を逐次処理して、計算結果４０８を例えばＨＤ１０６に格納する。計算結果はモニタ１０２、ＦＤ１０９、ネットワークＩ／

Ｆ１１４、プリンタ１１５などを通して出力される。

【００３６】

図５は、図４に示した構成を持つ情報処理装置１００におけるべき乗剰余演算の処理手順を説明するためのフローチャートである。例えば、ＣＰＵ１０３は、図３のフローチャートに対応する処理プログラムを読み出して実行する。これにより、情報処理装置１００は次のように動作する。

【００３７】

ステップＳ５００：

入力された入力値ｅ（ｋビット長）をΣｉ－０，…，ｋ－１２ｉ＊ｅ＿ｉ（ｅ＿ｉは０または１）のように２進表現しておく。入力値ｘ，Ｎ，ｅは例えばＨＤ１０６に格納される。

【００３８】

ステップＳ５０１：

入力値ｘ，Ｎから、候補指数格納部４０２にあるＬ個の候補指数｛ｌ＿ｉ｝（０≦ｉ≦Ｌ－１）のそれぞれに対し、ｘ＾｛ｌ＿ｉ｝を事前に計算し、事前計算数値格納部４０４に格納する。

【００３９】

ステップＳ５０２：

指数ｅ（ビット長ｋ）を候補指数｛ｌ＿ｉ｝のいずれかと一致するように複数の数値｛ｆ＿ｉ｝（０≦ｉ≦Ｆ－１）に分割する。このときｆ＿ｉのビット長をｂ＿ｉとすると、ｋ＝Σｉ－０，…，Ｆ－１ｂ＿ｉとなるように分割しておく。

【００４０】

ステップＳ５０３：

まず計算結果格納部４０７に、Ｃ：＝ｘ＾ｆ＿０（ｍｏｄ　Ｎ）とおく。さらにｆ＿ｉ（０≦ｉ≦Ｆ－１）ごとに次のような逐次処理を行う。

ｆｏｒ　ｉ＝１　ｔｏ　Ｆ－１

１）Ｃ：＝　Ｃ＾２＾ｂ＿ｉ（ｍｏｄ　Ｎ）

２）ｉｆ　ｆ＿ｉ≠０　ｔｈｅｎ　Ｃ：＝Ｃ　＊　ｘ＾ｆ＿ｉ　（ｍｏｄ　Ｎ）

【００４１】

ステップＳ５０４：

ステップＳ５０３で得られた出力値ｃ＝ｘ^{e}（ｍｏｄ　Ｎ）を外部に出力する。

【００４２】

図６、図７および図８はｅ＝１１０１１０１１１０００１０１０００１の場合の処理例を表す。図６はステップＳ５０１における加算鎖の形成方法をあらわしている。ｘ→ｘ^{2}→ｘ^{4}→ｘ^{5}→ｘ^{10}→ｘ^{20}→ｘ^{21}→ｘ^{42}→ｘ^{84}→ｘ^{85}→。。。という処理を経てｘ^{5}、ｘ^{21}、ｘ^{85}など候補指数｛ｌ＿ｉ｝のそれぞれに対する、ｘ＾ｌ＿ｉが計算される。図７はステップＳ５０２の処理に対応し、ｅをｆ＿０＝（１），ｆ＿１＝（１０１）などと分割していることを示している。図８はステップＳ５０３の処理に対応した計算過程を表している。

【００４３】

（第２の実施の形態）

上記第１の実施の形態では、候補指数として１［０１］$_{L}$の形式の数値のみ扱ったが、本実施形態では（１１）という数値も候補として扱うことによって、第１の実施の形態よりも計算量を減らすことを実現する。

【００４４】

図９は、第１の実施の形態と同様にｅ＝１１０１１０１１１０００１０１０００１の場合の処理例であり、ステップＳ５０１に相当する事前計算処理における加算鎖の形成方法をあらわしている。図６との違いは、ｘ→ｘ^{2}→ｘ^{4}→ｘ^{5}ではなくｘ→ｘ^{3}→ｘ^{5}と算出している点である。加算鎖が短くなったことに加え、図１０のようにｅの指数分割においても、分割後数値の個数を少なくすることができ、べき乗剰余演算の計算量を削減することができる。

【００４５】

（第３の実施の形態）

上記第１及び第２の実施の形態では、ｅの指数分割において、分割ビット列が重複するような分割を許していなかった。本実施形態では、分割する際にビット列中の（１０）を（０１）と（０１）の２つに分割することで計算量を削減する

ことを実現する。

【００４６】

図１１は、第１及び第２の実施の形態と同様にｅ＝１１０１１０１１１０００１０１０００１の場合の処理例である。ｅの先頭３ビット１１０のうち後半２ビット１０を２つの０１，０１に分割し、その片方を先頭１ビットに付加することで１０１を得る。分割されたもう片方の０１は、残りのビットに付加される。このような分割処理を繰り返すことにより候補指数の出現確率を高め、ステップＳ５０３の逐次処理回数を削減することができる。

【００４７】

このときステップＳ５０３で使用されるｂ＿ｉはｆ＿ｉのビット長をそのまま利用するのではなく、ｆ＿ｉどうしの重なりを考慮せねばならない。図１１においては、先頭７ビット（１１０１１０１）の分割は、ｆ＿０＝（１０１），ｂ＿０＝２，ｆ＿１＝（１０１０１），ｂ＿１＝１，ｆ＿２＝（１），ｂ＿２＝４となり、ｂ＿０＋ｂ＿１＋ｂ＿２＝７のようにビット長が一致するようにｂ＿ｉを定める必要がある。ｂ＿ｉはｆ＿ｉのビット長から次のｆ＿（ｉ＋１）との重なるビット長を引いた数を利用すればよい。

【００４８】

例として指数候補が｛（０），（１），（１１），（１０１）｝である場合の入力値ｅを処理する場合で説明する。指数の値に対するｆ＿ｉ，ｂ＿ｉの対と、変数ｓｈｔに格納される数値の表を図１２に示す。また、ｂ＿ｉを求める処理手順のフローチャートを図１３に示す。

【００４９】

ステップＳ１３０１では、入力値ｅの先頭３ビットにより処理が分類される。１１０および１１１の場合にはさらに１ビット分が読み込まれ、図１２に従って処理される。ステップＳ１３０２では図１３に記載されているとおりに分類ビット列としてｆ＿ｉとｂ＿ｉ　を追加し、前ステップＳ１３０１で３ビット読み込んだ場合には３ビット分、４ビット読み込んだ場合には４ビットシフトさせる。ステップＳ１３０３では処理ビットが１かどうかで処理を分岐し、０の場合にはステップＳ１３０４のように変数ｓｈｔを１つ増加させ１ビットシフトする。こ

の処理を先頭ビットが１になるまで繰り返し、ステップＳ１３０５を実行する。最終的にすべてのビットを読み込んだかどうかをステップＳ１３０６で判断し、読み終えた場合には終了する。分割されたｆ＿ｉ，ｂ＿ｉの処理はステップＳ５０３と同様であるため省略する。

【００５０】

（第４の実施の形態）

入力されたｅによっては事前計算処理が不要の場合が考えられる。例えばｅ＝３などビット長が小さい場合、もしくはｅ＝２＾１００など２進数表現したときに１が立っているビット数が少ない場合である。この問題に対処するために、入力値ｅに対して乗算計算回数を概算することで、事前計算が必要か不要かを選択することができ、ステップＳ５０１の処理を無くすことができる。また、ｅの分割方法が複数ある場合に、それぞれにおける乗算計算回数を概算して、どの分割方法を採用するかを選択するようにしてもよい。すなわち、概算された乗算計算回数により、指数を分割して計算するか否か、どのように分割するかを制御することができる。

【００５１】

また、乗算計算回数を概算する際に、乗算が２乗演算の場合とそうでない場合によって重み付けを行う方法も有効である。Ｈｉｇｈ－Ｓｐｅｅｄ　ＲＳＡ　Ｉｍｐｌｅｍｅｎｔａｔｉｏｎ，ＲＳＡ　Ｌａｂｏｒａｔｏｒｉｅｓ，１９９４によると、２乗演算は、異なる数値どうしの乗算にくらべ、計算量が少ないことが知られている。例えば、２乗演算の場合には０．８回、そうでない場合には１回とカウントする例が挙げられる。

【００５２】

（第５の実施の形態）

図１４は、図１の情報処理装置１００において、特徴とする機能（情報分散処理の機能）に着目して図示したものである。情報処理装置１００は、図１４に示すように、候補指数格納部４０２、事前計算モジュール４０３、事前計算数値格納部４０４、分割モジュール４０５、逐次処理モジュール４０６及び計算結果格納部４０７を有する。各モジュール４０３、４０５、４０７は、ＣＰＵ１０３が

所定のプログラムを実行することで実現される機能単位（モジュール）を表わす。

【００５３】

情報処理装置１００に対しては、外部から入力値ｘ、Ｎ（４００）及びｅ（４０１）が入力される。情報処理装置１００は、入力値からべき乗剰余演算を行い結果としてｃ＝ｘ^{e}（ｍｏｄ　Ｎ）（４０８）を出力する装置である。入力値Ｎが入力されない場合にはｃ＝べき乗演算ｘ^{e}を行うが、これはべき乗剰余演算の特殊な場合と考えられるため、第５の実施の形態では、べき乗剰余演算ｘ^{e}（ｍｏｄ　Ｎ）を行う装置の説明のみを行う。

【００５４】

候補指数格納部４０２には、あらかじめ、｛（０），（１），（１１），（１０１），（１０１１），（１１０１），（１０１０１），（１０１０１１），（１１０１０１），…｝（２進数表示）のように１［０１］$_{L}$または１１［０１］$_{L}$または１［０１］$_{L}$１（ただし［ｘｙ］$_{i}$はｉ回ｘｙを繰り返したもの）の形式を持つ数値が含まれている。

【００５５】

事前計算モジュール４０３は、入力値（４００）と候補指数格納部４０２から事前計算を行い、事前計算結果を、例えばＨＤ１０６にある、事前計算数値格納部４０４に格納する。分割モジュール４０５は、入力値４０１を分割し、入力値４０１および分割された数値を、例えばＨＤ１０６に格納する。逐次処理モジュール４０６は、例えばＨＤ１０６にある計算結果格納部４０７を逐次処理して、計算結果４０８を例えばＨＤ１０６に格納する。計算結果はモニタ１０２、ＦＤ１０９、ネットワークＩ／Ｆ１１４、プリンタ１１５などを通して出力される。

【００５６】

図１４に示した構成による情報処理装置１００の動作における情報分散処理の手順は、図５に示したフローチャートに従う。例えば、ＣＰＵ１０３は、図５のフローチャートに従った処理プログラムを読み出して実行する。これにより、情報処理装置１００は次のように動作する。

【００５７】

ステップＳ５００：

入力された入力値ｅ（ｋビット長）を$\Sigma_{i=0,\cdots,k-1} 2^i * e_i$（ｅ＿ｉは０または１）のように２進表現しておく。入力値ｘ，Ｎ，ｅは例えばＨＤ１０６に格納される。

【００５８】

ステップＳ５０１：

入力値ｘ，Ｎから、候補指数格納部４０２にあるＬ個の候補指数｛ｌ＿ｉ｝（０≦ｉ≦Ｌ－１）のそれぞれに対し、ｘ＾ｌ＿ｉ　を事前に計算し、事前計算数値格納部４０４に格納する。

【００５９】

事前計算数値格納部４０４の内部には、計算後結果を格納するための$F_1()$，$F_2()$，$F_3()$，$F_4()$の４つの配列領域４１１～４１４（それぞれの配列の長さはＱ）が用意されている。図１８は、４１１～４１４の配列領域に値を格納する処理手順を示すフローチャートである。

【００６０】

まず、ステップＳ９０１により、それぞれの配列領域には$F_1(0)=x$，$F_2(0)=1$，$F_3(0)=x$，$F_4(0)=x$が初期値として設定され、変数ｉに０が格納される。

【００６１】

次にステップＳ９０２により、$F_1(i)=F_2(i-1)*F_4(i-1) \pmod N$が格納される。同様にステップＳ９０３により$F_2(i)=F_1(i)*F_3(i-1) \pmod N$，ステップＳ９０４により$F_3(i)=F_2(i)*F_3(i-1) \pmod N$，ステップＳ９０５により$F_4(i)=F_1(i)*F_2(i) \pmod N$が格納され、ステップＳ９０６により変数ｉがＱ－１と一致するかどうか判定する。一致しない場合はステップＳ９０７で変数ｉを１つ増加させて、ステップＳ９０２に戻る。一致する場合は終了である。

【００６２】

また、ステップＳ９０４とステップＳ９０５は、逐次的に行うのではなく、並

列処理させることが可能であり、並列処理を行うことで高速化が可能である。

【００６３】

ステップＳ５０２：

指数ｅ（ビット長ｋ）を候補指数｛ｌ＿ｉ｝のいずれかと一致するように複数の数値｛ｆ＿ｉ｝（０≦ｉ≦Ｆ－１）に分割する。このときｆ＿ｉのビット長をｂ＿ｉとすると、ｋ＝Σｉ－０，…，Ｆ－１ｂ＿ｉとなるように分割しておく。

【００６４】

ステップＳ５０３：

まず計算結果格納部４０７に、Ｃ：＝ｘ＾ｆ＿０（ｍｏｄ　Ｎ）とおく。さらにｆ＿ｉ（０≦ｉ≦Ｆ－１）ごとに次のような逐次処理を行う。

ｆｏｒ　ｉ＝１　ｔｏ　Ｆ－１

１）Ｃ：＝Ｃ＾２＾ｂ＿ｉ（ｍｏｄ　Ｎ）

２）ｉｆ　ｆ＿ｉ≠０　ｔｈｅｎ　Ｃ：＝Ｃ　＊　ｘ＾ｆ＿ｉ　（ｍｏｄ　Ｎ）

【００６５】

ステップＳ５０４：

ステップＳ５０３で得られた出力値ｃ＝ｘ^{e}（ｍｏｄ　Ｎ）を外部に出力する。

【００６６】

図１５は、本実施形態における加算鎖の構成方法を表している。前述のように、候補指数は２進数表示したとき１［０１］$_{L}$または１１［０１］$_{L}$または１［０１］$_{L}$１（ただし［ｘｙ］$_{i}$はｉ回ｘｙを繰り返したもの）の形式を持つが、これらの候補指数を効率的に算出する方法を以下に示す。

【００６７】

$f_1()$，$f_2()$，$f_3()$，$f_4()$の４つの関数は$f_1(0)=1$，$f_2(0)=0$，$f_3(0)=1$，$f_4(0)=1$を初期値として$f_1(i)=f_2(i-1)+f_4(i-1)$，$f_2(i)=f_1(i)+f_3(i-1)$，$f_3(i)=f_2(i)+f_3(i-1)$，$f_4(i)=f_1(i)+f_2(i)$

を満たすように循環的に計算を行っていく。計算順序は、f_1（1）→f_2（1）→f_3（1）→f_4（1）→f_1（2）→f_2（2）→f_3（2）→f_4（2）→…のように行う。このとき、f_1（i）＝1［01］$_i$，f_2（i）＝10［00］$_i$，f_3（i）＝11［01］$_i$，f_4（i）＝1［01］$_i$1という形式となる。このようにして、｛1，2，3，5，8，11，13，21，32，43，53，85，128，171，213，314，…｝という加算鎖を構成することができる。

【0068】

図16および図17は、候補指数の最大ビット長W＝4（つまり指数候補は｛（1），（11），（101），（1011），（1101）｝である），e＝1101101110001010001の場合の処理例を表す。まずステップS501に対応して、候補指数｛l__i｝のそれぞれに対する、$x^{l__i}$が計算される。図7はステップS502の処理に対応し、eをf__0＝（1101），f__1（1011），f__2＝（11）などと分割していることを示している。図8はステップS503の処理に対応した計算過程を表している。

【0069】

（第6の実施の形態）

上記第5の実施の形態では、eの指数分割において、分割ビット列が重複するような分割を許していなかったが、第3の実施の形態と同様に、分割する際にビット列中の（10）を（01）と（01）の2つに分割することで計算量を削減することが実現できる。図19は、図12の表及び図13記載のフローチャートを用いて、e＝1111101110001101001111を分割した例である。

【0070】

（その他の実施の形態）

本発明は、複数の機器（例えばホストコンピュータ等）から構成されるシステムの一部として適用しても、一つの機器からなるものの一部に適用してもよい。

【0071】

また、上述した実施の形態の機能を実現するべく各種のデバイスを動作させる

ように、該各種デバイスと接続された装置或いはシステム内のコンピュータに対し、上記実施の形態の機能を実現するためのソフトウェアのプログラムコードを供給し、そのシステム或いは装置のコンピュータ（ＣＰＵ或いはＭＰＵ）に格納されたプログラムに従って上記各種デバイスを動作させることによって実施したものも、本発明の範疇に含まれる。

【００７２】

また、この場合、上記ソフトウェアのプログラムコード自体が上述した実施の形態の機能を実現することになり、そのプログラムコード自体は本発明を構成する。そのプログラムコードの伝送媒体としては、プログラム情報を搬送波として伝搬させて供給するためのコンピュータネットワーク（ＬＡＮ、インターネット等のＷＡＮ、無線通信ネットワーク等）システムにおける通信媒体（光ファイバ等の有線回線や無線回線等）を用いることができる。

【００７３】

さらに、上記プログラムコードをコンピュータに供給するための手段、例えばかかるプログラムコードを格納した記録媒体は本発明を構成する。かかるプログラムコードを記憶する記録媒体としては、例えばフレキシブルディスク、ハードディスク、光ディスク、光磁気ディスク、ＣＤ－ＲＯＭ、磁気テープ、不揮発性のメモリカード、ＲＯＭ等を用いることができる。

【００７４】

また、コンピュータが供給されたプログラムコードを実行することにより、上述の実施の形態の機能が実現されるだけでなく、そのプログラムコードがコンピュータにおいて稼働しているＯＳ（オペレーティングシステム）或いは他のアプリケーションソフト等と共同して上述の実施の形態の機能が実現される場合にもかかるプログラムコードは本発明の実施の形態に含まれることはいうまでもない。

【００７５】

さらに、供給されたプログラムコードがコンピュータの機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに格納された後、そのプログラムコードの指示に基づいてその機能拡張ボードや機能拡張ユニットに備わ

るＣＰＵ等が実際の処理の一部又は全部を行い、その処理によって上述した実施の形態の機能が実現される場合にも本発明に含まれることはいうまでもない。

【００７６】

以下、上記実施形態に係わる本発明の特徴を整理する。

【００７７】

特徴１．

２つの整数ｘおよびｅからｘｅを計算するべき乗演算装置において、

２つの整数ｘおよびｅを入力する入力手段と、

Ｌ個の候補指数｛ｌ＿ｉ｝（０≦ｉ≦Ｌ－１）を格納する候補指数格納手段と、

前記候補指数格納手段に格納されている候補指数｛ｌ＿ｉ｝のそれぞれに対し、入力された整数ｘからｘ＾｛ｌ＿ｉ｝を事前に計算しておく事前計算手段と、

事前計算された数値ｘ＾｛ｌ＿ｉ｝を格納する事前計算数値格納手段と、

入力された整数ｅを前記候補指数｛ｌ＿ｉ｝のいずれかと一致するように複数の数値｛ｆ＿ｉ｝（０≦ｉ≦Ｆ－１）に分割する分割手段と、

計算結果ｃを格納する計算結果格納手段と、

分割された数値｛ｆ＿ｉ｝（０≦ｉ≦Ｆ－１）について、事前計算された数値ｘ＾｛ｌ＿ｉ｝を用いて計算結果ｃを逐次更新する逐次処理手段と、

全ての前記数値｛ｆ＿ｉ｝について更新後の計算結果ｃをｘｅとして出力する出力手段と

を有することを特徴とするべき乗演算装置。

【００７８】

特徴２．

３つの整数ｘ、ｅおよびＮからｘｅ（ｍｏｄ　Ｎ）を計算するべき乗演算装置において、

３つの整数ｘ、ｅおよびＮを入力する入力手段と、

Ｌ個の候補指数｛ｌ＿ｉ｝（０≦ｉ≦Ｌ－１）を格納する候補指数格納手段と、

前記候補指数格納手段に格納されている候補指数｛ｌ＿ｉ｝のそれぞれに対し

、入力された整数ｘからｘ＾｛ｌ＿ｉ｝を事前に計算しておく事前計算手段と、

事前計算された数値ｘ＾｛ｌ＿ｉ｝を格納する事前計算数値格納手段と、

入力された整数ｅを前記候補指数｛ｌ＿ｉ｝のいずれかと一致するように複数の数値｛ｆ＿ｉ｝（０≦ｉ≦Ｆ－１）に分割する分割手段と、

計算結果ｃを格納する計算結果格納手段と、

分割された数値｛ｆ＿ｉ｝（０≦ｉ≦Ｆ－１）について、事前計算された数値ｘ＾｛ｌ＿ｉ｝を用いて計算結果ｃを逐次更新する逐次処理手段と、

全ての前記数値｛ｆ＿ｉ｝について更新後の計算結果ｃをｘ^{e}　（ｍｏｄ　Ｎ）として出力する出力手段と

を有することを特徴とするべき乗演算装置。

【００７９】

特徴３．

前記逐次処理手段は、

前記計算結果格納手段内に、前記計算結果ｃの初期値としてｆ＿０を設定する初期化手段と、

前記分割数値｛ｆ＿ｉ｝（１≦ｉ≦Ｆ－１）のそれぞれにつき、ｆ＿ｉを２進数表示したときのビット長分ｃ：＝ｃ^{2}の更新処理を行い、さらにｃ：＝ｃ＊ｆ＿Ｉの更新処理を行う更新処理手段と

を有することを特徴とする特徴１または２に記載の情報処理装置。

【００８０】

特徴４．

前記候補指数格納手段に格納される候補指数は、２進数表示が（０）または１［０１］$_{L}$（ただし［ｘｙ］$_{i}$はｉ回ｘｙを繰り返したもの）の形式であることを特徴とする特徴１または２に記載の情報処理装置。

【００８１】

特徴５．

前記候補指数格納手段に格納された候補指数は、２進数表示が、（０）または（１１）または１［０１］$_{L}$（ただし［ｘｙ］$_{i}$はｉ回ｘｙを繰り返したもの）の形式であることを特徴とする特徴１または２に記載の情報処理装置。

【００８２】

特徴６．

前記分割手段は、分割後数値を２進数表示したとき、ビット列中の（１０）を（０１）と（０１）の２つに分割して、｛ｆ＿ｉ｝の重複を許す分割方法であり、

前記逐次処理手段におけるｃ：＝ｃ^{2}の更新処理を、ｆ＿ｉのビット長分行うのではなく、重複しているビット列の長さ分は更新処理を行わないことを特徴とする特徴１または２に記載の情報処理装置。

【００８３】

特徴７．

前記分割手段による分割に応じた乗算回数を概算する乗算回数概算手段と、

当該概算された乗算回数に基づいて、前記分割手段による分割を制御する分割制御手段とを有することを特徴とする特徴１または２に記載の情報処理装置。

【００８４】

特徴８．

前記乗算回数概算手段は、異なる２値の乗算と同一値同士の乗算とで、異なる重みをつけて乗算回数を概算することを特徴とする特徴７に記載の情報処理装置。

【００８５】

特徴９．

前記候補指数格納手段に格納される候補指数の個数Ｌを、入力値ｅのビット長により増減させることを特徴とする特徴１または２に記載の情報処理装置。

【００８６】

特徴１０．

前記候補指数格納手段に格納された候補指数は、０であるかまたは、２進数表示でＷビット数以下であって、１［０１］$_{L}$（ただし［ｘｙ］$_{i}$はｘｙをｉ回繰り返したもの）の形式であるか、１１［０１］$_{L}$の形式であるか、または１［０１］$_{L}$１の形式であることを特徴とする特徴１または２に記載の情報処理装置。

【００８７】

特徴１１．

前記事前計算手段は、

候補指数を表現する$f_1()$，$f_2()$，$f_3()$，$f_4()$の４つの関数を利用し、

$f_1(0)=1$，$f_2(0)=0$，$f_3(0)=1$，$f_4(0)=1$を初期値として

$f_1(i)=f_2(i-1)+f_4(i-1)$，$f_2(i)=f_1(i)+f_3(i-1)$，$f_3(i)=f_2(i)+f_3(i-1)$，$f_4(i)=f_1(i)+f_2(i)$を満たすように循環的に計算を行うことで、$f_1(i)=1[01]_i$，$f_2(i)=10[00]_i$，$f_3(i)=11[01]_i$，$f_4(i)=1[01]_i1$という形式を得ることで加算鎖を構成し、

$xf2(i-1)$と$xf4(i-1)$の積から$xf1(i)$を、$xf1(i)$と$xf3(i-1)$の積から$xf2(i)$を、$xf2(i)$と$xf3(i-1)$の積から$xf3(i)$を、$xf1(i)$と$xf2(i)$の積から$xf4(i)$を計算し、

当該計算結果を前記計算結果格納手段に格納することを特徴とする特徴１０に記載の情報処理装置。

【００８８】

特徴１２．

前記計算結果格納手段は、

計算後結果を格納する$F_1()$，$F_2()$，$F_3()$，$F_4()$の４つの配列領域を持ち、

$F_1(0)=x$，$F_2(0)=1$，$F_3(0)=x$，$F_4(0)=x$を初期値として設定し、

前記事前計算手段は、

$F_1(i)=F_2(i-1)*F_4(i-1)$，$F_2(i)=F_1(i)*F_3(i-1)$，$F_3(i)=F_2(i)*F_3(i-1)$，$F_4(i)=F_1(i)*F_2(i)$を満たすように循環的に計算し、

当該計算結果を前記計算結果格納手段に格納することを特徴とする特徴１０に

記載の情報処理装置。

【００８９】

特徴１３．

前記候補指数格納手段に格納される候補指数は、前記整数ｅのビット数に応じてＷを変化させることを特徴とする特徴１０に記載の情報処理装置。

【００９０】

特徴１４．

２つの整数ｘおよびｅからｘｅを計算するべき乗演算方法において、

２つの整数ｘおよびｅを入力する入力工程と、

候補指数格納部に格納されているＬ個の候補指数｛ｌ＿ｉ｝（０≦ｉ≦Ｌ－１）のそれぞれに対し、入力された整数ｘからｘ＾｛ｌ＿ｉ｝を事前に計算して事前計算数値格納部に格納しておく事前計算工程と、

入力された整数ｅを前記候補指数｛ｌ＿ｉ｝のいずれかと一致するように複数の数値｛ｆ＿ｉ｝（０≦ｉ≦Ｆ－１）に分割する分割工程と、

分割された数値｛ｆ＿ｉ｝（０≦ｉ≦Ｆ－１）について、事前計算された数値ｘ＾｛ｌ＿ｉ｝を用いて、計算結果格納部に格納されている計算結果ｃを逐次更新する逐次処理工程と、

全ての前記数値｛ｆ＿ｉ｝について更新後の計算結果ｃをｘｅとして出力する出力工程と

を有することを特徴とするべき乗演算方法。

【００９１】

特徴１５．

３つの整数ｘ、ｅおよびＮからｘｅ（ｍｏｄ　Ｎ）を計算するべき乗演算方法において、

３つの整数ｘ、ｅおよびＮを入力する入力工程と、

候補指数格納部に格納されているＬ個の候補指数｛ｌ＿ｉ｝（０≦ｉ≦Ｌ－１）のそれぞれに対し、入力された整数ｘからｘ＾｛ｌ＿ｉ｝を事前に計算して事前計算数値格納部に格納しておく事前計算工程と、

入力された整数ｅを前記候補指数｛ｌ＿ｉ｝のいずれかと一致するように複数

の数値｛ｆ＿ｉ｝（０≦ｉ≦Ｆ－１）に分割する分割工程と、

分割された数値｛ｆ＿ｉ｝（０≦ｉ≦Ｆ－１）について、事前計算された数値ｘ＾｛ｌ＿ｉ｝を用いて、計算結果格納部に格納されている計算結果ｃを逐次更新する逐次処理工程と、

全ての前記数値｛ｆ＿ｉ｝について更新後の計算結果ｃをｘｅ　（ｍｏｄ　Ｎ）として出力する出力工程と

を有することを特徴とするべき乗演算方法。

【００９２】

特徴１６．

２つの整数ｘおよびｅからｘｅを計算するべき乗演算をコンピュータに実行させるためのコンピュータ読み取り可能なプログラムにおいて、

２つの整数ｘおよびｅを入力する入力工程と、

候補指数格納部に格納されているＬ個の候補指数｛ｌ＿ｉ｝（０≦ｉ≦Ｌ－１）のそれぞれに対し、入力された整数ｘからｘ＾｛ｌ＿ｉ｝を事前に計算して事前計算数値格納部に格納しておく事前計算工程と、

入力された整数ｅを前記候補指数｛ｌ＿ｉ｝のいずれかと一致するように複数の数値｛ｆ＿ｉ｝（０≦ｉ≦Ｆ－１）に分割する分割工程と、

分割された数値｛ｆ＿ｉ｝（０≦ｉ≦Ｆ－１）について、事前計算された数値ｘ＾｛ｌ＿ｉ｝を用いて、計算結果格納部に格納されている計算結果ｃを逐次更新する逐次処理工程と、

全ての前記数値｛ｆ＿ｉ｝について更新後の計算結果ｃをｘｅとして出力する出力工程と

を有することを特徴とするプログラム。

【００９３】

特徴１７．

３つの整数ｘ、ｅおよびＮからｘｅ（ｍｏｄ　Ｎ）を計算するべき乗演算をコンピュータに実行させるためのコンピュータ読み取り可能なプログラムにおいて、

３つの整数ｘ、ｅおよびＮを入力する入力工程と、

候補指数格納部に格納されているＬ個の候補指数｛ｌ＿ｉ｝（０≦ｉ≦Ｌ－１）のそれぞれに対し、入力された整数ｘからｘ＾｛ｌ＿ｉ｝を事前に計算して事前計算数値格納部に格納しておく事前計算工程と、

入力された整数ｅを前記候補指数｛ｌ＿ｉ｝のいずれかと一致するように複数の数値｛ｆ＿ｉ｝（０≦ｉ≦Ｆ－１）に分割する分割工程と、

分割された数値｛ｆ＿ｉ｝（０≦ｉ≦Ｆ－１）について、事前計算された数値ｘ＾｛ｌ＿ｉ｝を用いて、計算結果格納部に格納されている計算結果ｃを逐次更新する逐次処理工程と、

全ての前記数値｛ｆ＿ｉ｝について更新後の計算結果ｃをｘｅ　（ｍｏｄ　Ｎ）として出力する出力工程と

を有することを特徴とするプログラム。

【００９４】

【発明の効果】

以上説明したように本発明によれば、ｅを２進数表示した際のビット列内にある特徴を持つビット列が登場することを想定して、それらのビット列を候補指数として、それらに関してのみ事前計算を行うことで、事前計算処理量を削減し、従来方式に比べて少ない演算回数で計算することができるべき乗計算方式を提供することができる。

【００９５】

また事前計算しておく数値の数が少なくなるので、事前計算数値を記憶するためのテーブルサイズをおさえるメリットもあわせ持ち、テーブル参照のためのメモリ領域を削減することができる。

【図面の簡単な説明】

【図１】

実施形態の情報処理装置の構成を示すブロック図である。

【図２】

従来例であるＢｉｎａｒｙ　Ｍｅｔｈｏｄでの処理を表す図である。

【図３】

従来例であるＱｕａｔｅｒｎａｒｙ　Ｍｅｔｈｏｄでの処理を表す図である。

【図４】

第１の実施の形態における情報処理装置の機能構成を示すブロック図である。

【図５】

第１の実施の形態におけるべき乗剰余演算の処理手順を説明するためのフローチャートである。

【図６】

第１の実施の形態における加算鎖の形成方法を表す図である。

【図７】

第１の実施の形態における指数分割の例を示す図である。

【図８】

第１の実施の形態における逐次計算の例を示す図である。

【図９】

第２の実施の形態における加算鎖の形成方法を表す図である。

【図１０】

第２の実施の形態における指数分割の例を示す図である。

【図１１】

第３の実施の形態における指数分割の例を示す図である。

【図１２】

指数の値に対するｆ＿ｉ，ｂ＿ｉの対と、変数ｓｈｔに格納される数値の表を表す図である。

【図１３】

ｂ＿ｉを求める処理手順を示すフローチャートである。

【図１４】

第５の実施の形態における情報処理装置の機能構成を示すブロック図である。

【図１５】

第５の実施の形態における加算鎖の形成方法を表す図である。

【図１６】

第５の実施の形態における指数分割の例を示す図である。

【図１７】

第５の実施の形態における逐次計算の例を示す図である。

【図１８】

配列領域に値を格納する処理手順を示すフローチャートである。

【図１９】

第６の実施の形態における指数分割の例を示す図である。

【符号の説明】

１００　情報処理装置

１０２　モニタ

１０３　ＣＰＵ

１０４　ＲＯＭ

１０５　ＲＡＭ

１０６　ＨＤ

１０７　ネットワーク接続部

１０８　ＣＤドライブ

１０９　ＦＤドライブ

１１０　ＤＶＤドライブ

１１１　インターフェース

１１２　マウス

１１３　キーボード

１１４　インターフェース

１１５　プリンタ

１１６　バス

１１７　インターフェース

１１８　モデム

１１９　インターフェース

４００　入力値　ｘ、Ｎ

４０１　入力値　ｅ

４０２　候補指数格納部

４０３　事前計算モジュール

４０４　事前計算数値格納部

４０５　分割モジュール

４０６　逐次処理モジュール

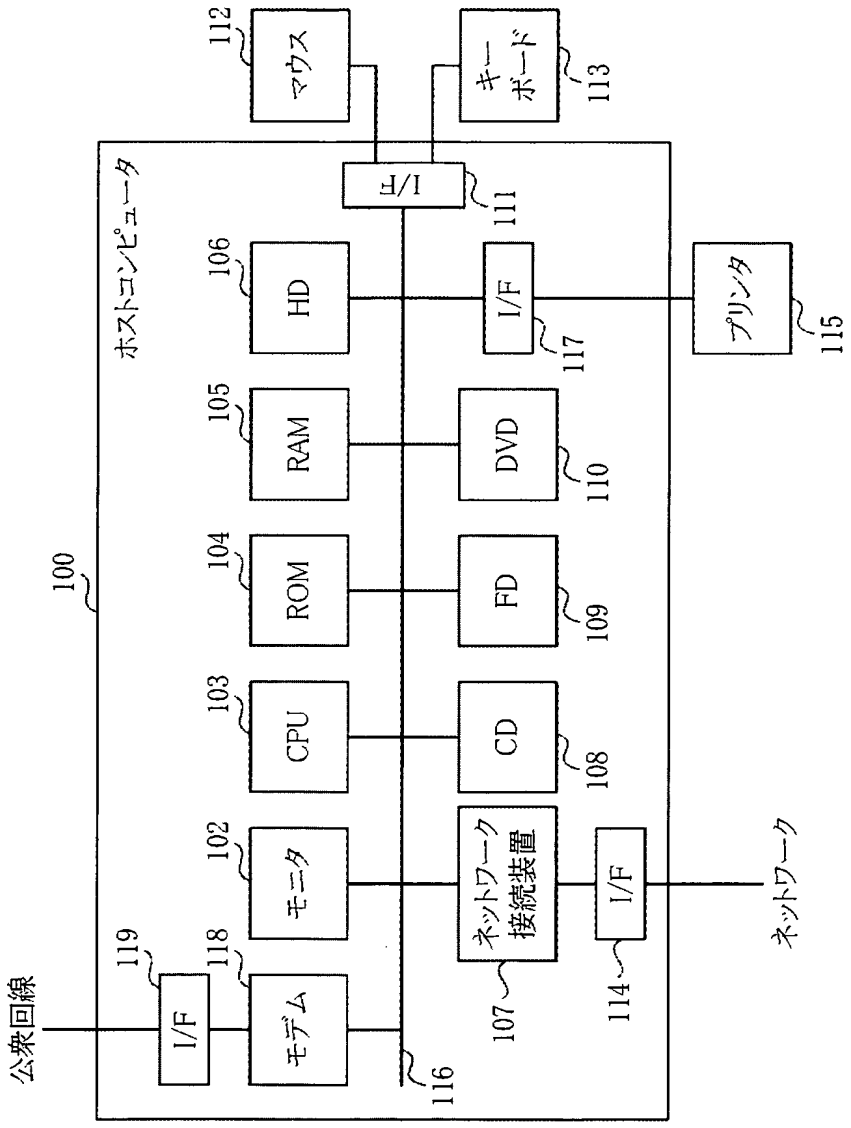
４０７　計算結果格納部

４０８　計算結果　ｃ

４１１～４１４　配列領域

【書類名】　図面

【図１】


ホストコンピュータ
100
CPU
103
ROM
104
RAM
105
HD
106
FD
109
CD
108
DVD
110
I/F
111
マウス
112
キーボード
113
I/F
117
プリンタ
115
ネットワーク接続装置
107
I/F
114
ネットワーク
モニタ
102
モデム
118
I/F
119
公衆回線
116

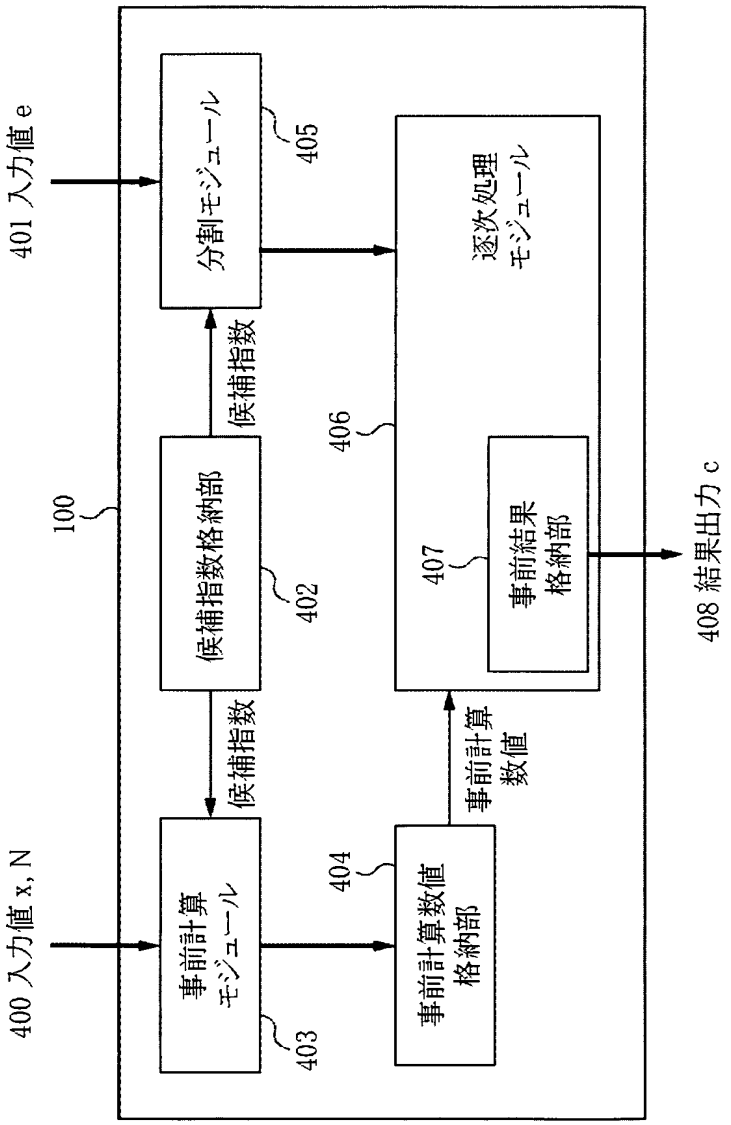
【図２】

	処理2-1)	処理2-2)
1		x
1	$(x)^2=x^2$	$x^2 \cdot x=x^3$
0	$(x^3)^2=x^6$	x^6
1	$(x^6)^2=x^{12}$	$x^{12} \cdot x=x^{13}$
1	$(x^{13})^2=x^{26}$	$x^{26} \cdot x=x^{27}$
1	$(x^{27})^2=x^{54}$	$x^{54} \cdot x=x^{55}$

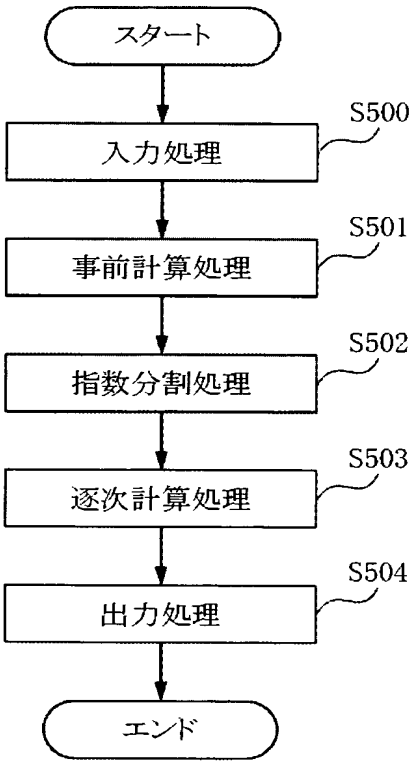
【図３】

	処理2-1)	処理2-2)
11		x^3
01	$(x^3)^4=x^{12}$	$x^{12}\cdot x=x^{13}$
11	$(x^{13})^4=x^{52}$	$x^{52}\cdot x^3=x^{55}$

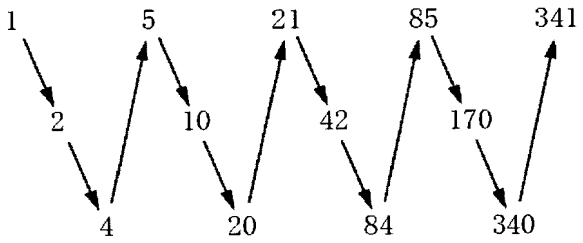
【図４】


400 入力値 x, N
401 入力値 e
100
事前計算モジュール
403
候補指数
候補指数格納部
402
分割モジュール
405
候補指数
406
逐次処理モジュール
事前結果格納部
407
408 結果出力 c
404
事前計算数値格納部
事前計算数値

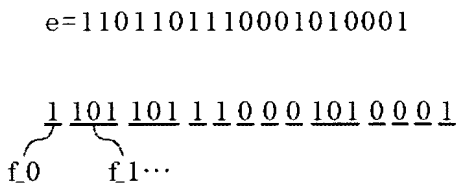
【図５】


スタート
S500
入力処理
S501
事前計算処理
S502
指数分割処理
S503
逐次計算処理
S504
出力処理
エンド

【図６】



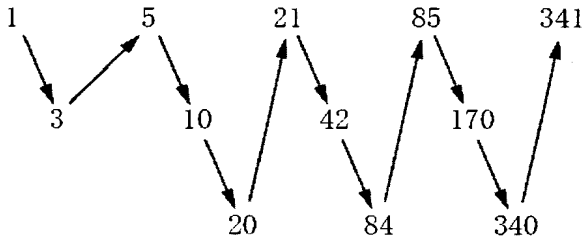
【図７】



【図８】

	ステップS503処理1)	処理2)
1		x^1
101	$(x^1)^8=x^8$	$x^8 \cdot x^5=x^{13}$
101	$(x^{13})^8=x^{104}$	$x^{104} \cdot x^5=x^{109}$
1	$(x^{109})^2=x^{218}$	$x^{218} \cdot x^1=x^{219}$
1	$(x^{219})^2=x^{438}$	$x^{438} \cdot x^1=x^{439}$
0	$(x^{439})^2=x^{878}$	$=x^{878}$

【図９】

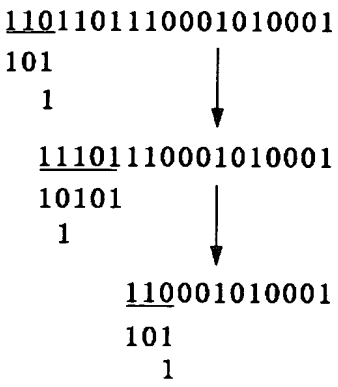


【図１０】

e=1101101110001010001

1 101 101 11 0 0 0 101 0 0 0 1

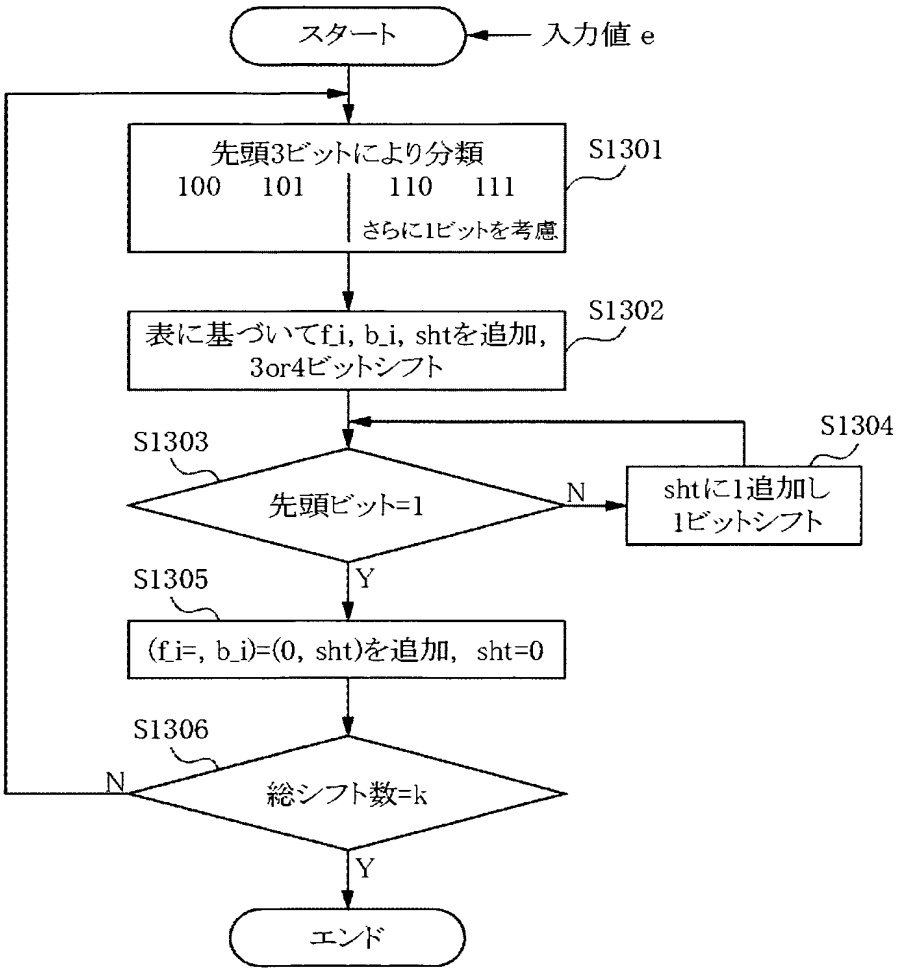
【図１１】


110110111000101000 1
101
1
11101110001010001
10101
1
110001010001
101
1

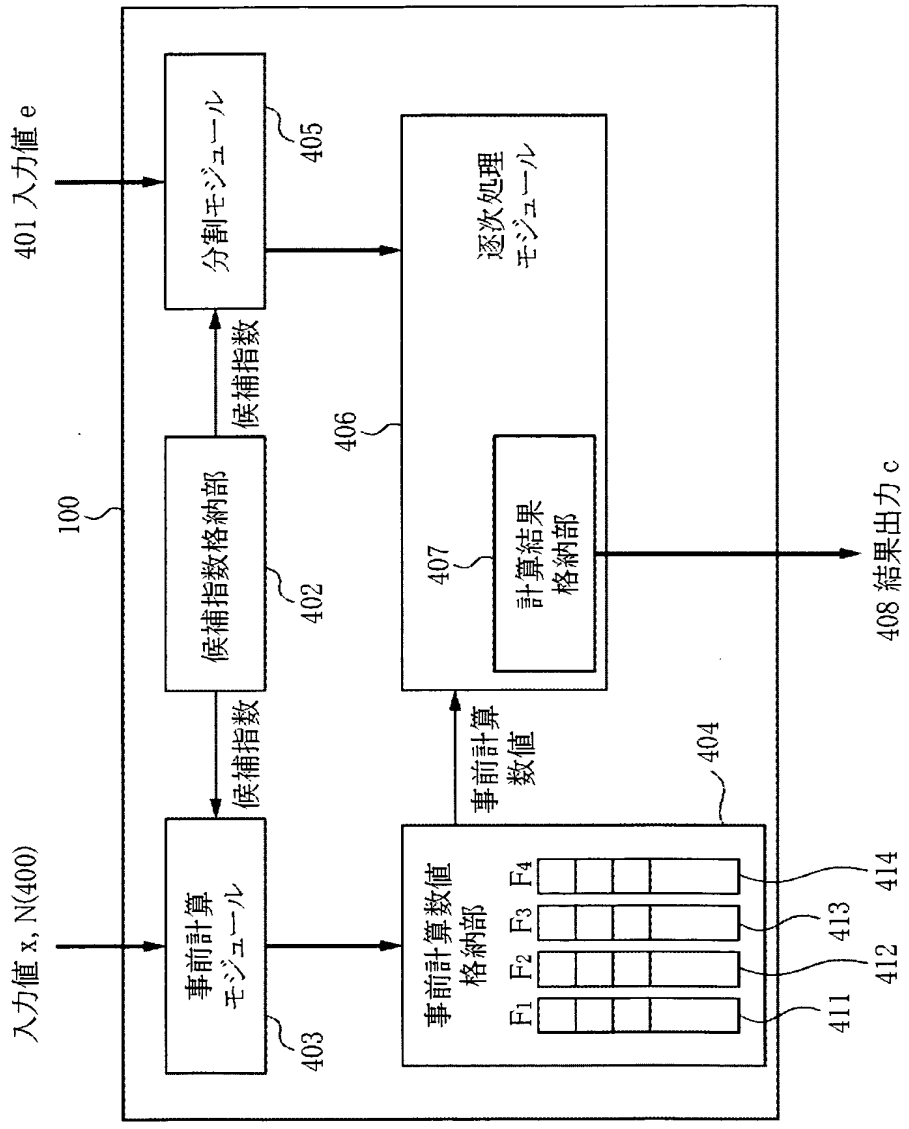
【図１２】

		f_i ,b_i	f_(i+1), b_(i+1)	sft
100		1 , 1	—	2
101		101, 3	—	0
110	0	11 , 2	—	2
	1	1 , 1	101,3	0
111	0	101, 1	1, 1	2
	1	101, 1	101, 3	0

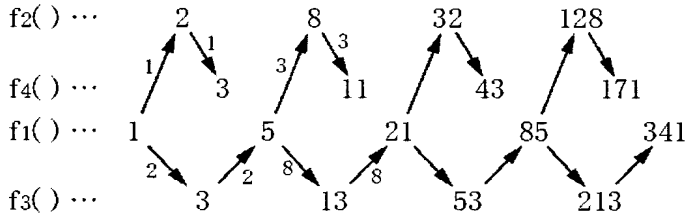
【図１３】


スタート
入力値 e
先頭3ビットにより分類
100　101　110　111
さらに1ビットを考慮
S1301
表に基づいてf_i, b_i, shtを追加,
3or4ビットシフト
S1302
S1303
先頭ビット=1
N
shtに1追加し
1ビットシフト
S1304
Y
S1305
(f_i=, b_i)=(0, sht)を追加, sht=0
S1306
N
総シフト数=k
Y
エンド

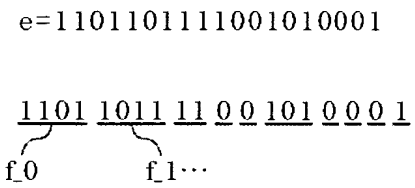
【図１４】


401 入力値 e
分割モジュール
405
候補指数
逐次処理
モジュール
406
100
候補指数格納部
402
407
計算結果
格納部
408 結果出力 c
候補指数
事前計算
数値
404
入力値 x, N(400)
事前計算
モジュール
403
事前計算数値
格納部
F1 F2 F3 F4
414
413
412
411

【図１５】



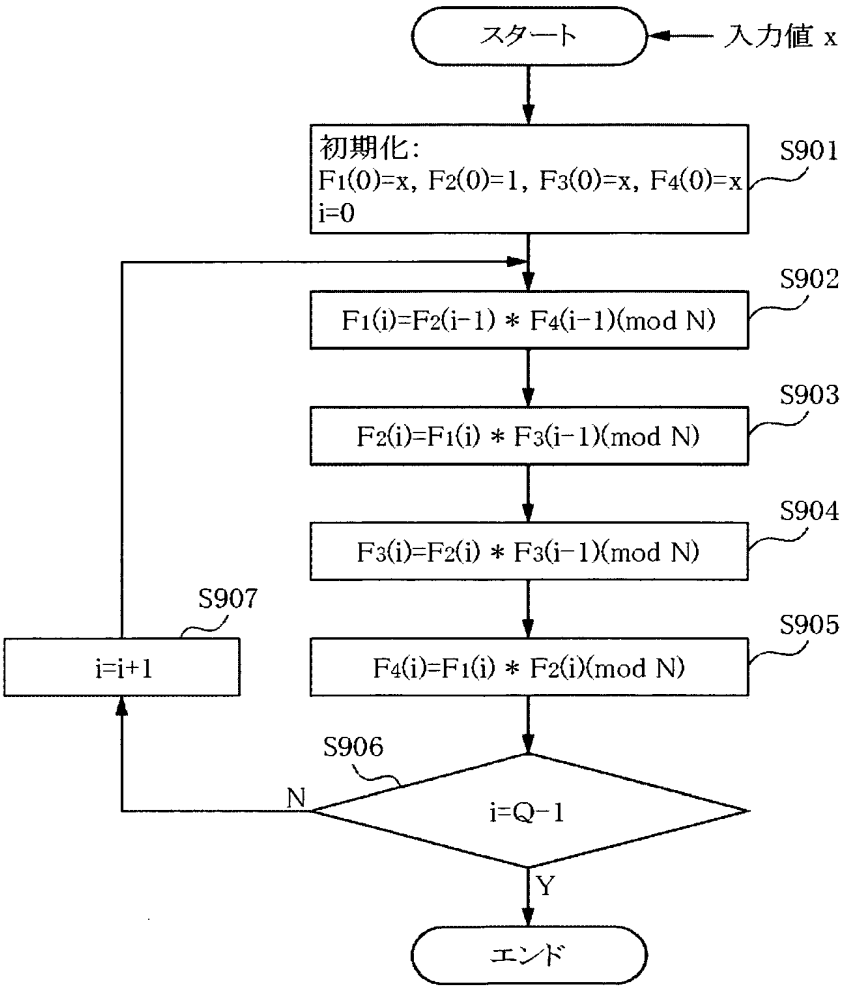
【図１６】



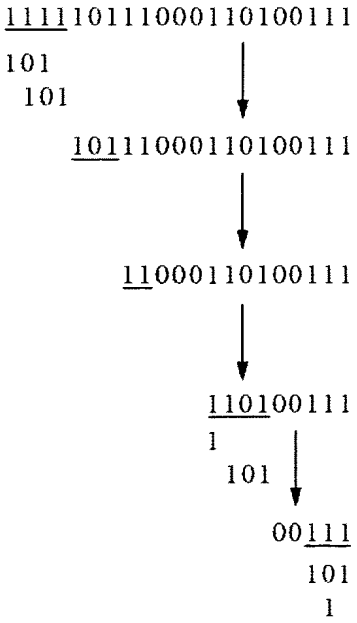
【図１７】

	ステップS503処理1)	処理2)
1101		x^{13}
1011	$(x^{13})^{16}=x^{208}$	$x^{208}\cdot x^{11}=x^{219}$
11	$(x^{219})^{4}=x^{876}$	$x^{876}\cdot x^{3}=x^{879}$
0	$(x^{879})^{2}=x^{1758}$	$=x^{1758}$
0	$(x^{1758})^{2}=x^{3516}$	$=x^{3516}$
101	$(x^{3516})^{8}=x^{28128}$	$x^{28128}\cdot x^{5}=x^{28133}$
…	…	…

【図１８】


スタート
入力値 x
初期化:
F1(0)=x, F2(0)=1, F3(0)=x, F4(0)=x
i=0
S901
S902
F1(i)=F2(i-1) * F4(i-1)(mod N)
S903
F2(i)=F1(i) * F3(i-1)(mod N)
S904
F3(i)=F2(i) * F3(i-1)(mod N)
S905
F4(i)=F1(i) * F2(i)(mod N)
S906
i=Q-1
N
Y
S907
i=i+1
エンド

【図１９】


1111101110001101001 11
101
101
1011100011010011 11
11000110100111
110100111
1
101
00111
101
1

【書類名】　　要約書

【要約】

【課題】　事前計算処理量とテーブルサイズを低減させ、少ない演算回数で計算できるべき乗演算装置を提供する。

【解決手段】　入力された２つの整数ｘおよびｅからｘｅを計算するべき乗演算装置において、候補指数格納部４０２に格納されたＬ個の候補指数｛ｌ＿ｉ｝（０≦ｉ≦Ｌ－１）のそれぞれに対し、事前計算モジュール４０３によりｘ＾｛ｌ＿ｉ｝を事前に計算して事前計算数値格納部４０４に格納しておき、分割モジュール４０５によりｅを候補指数｛ｌ＿ｉ｝のいずれかと一致するように複数の数値｛ｆ＿ｉ｝（０≦ｉ≦Ｆ－１）に分割し、逐次処理モジュール４０６により、｛ｆ＿ｉ｝について、計算結果格納部４０７に格納された計算結果ｃをｘ＾｛ｌ＿ｉ｝を用いて逐次更新し、全ての｛ｆ＿ｉ｝について更新後の計算結果ｃをｘｅとして出力する。

【選択図】　　図４

特願２００２－３１４５９５

出　願　人　履　歴　情　報

識別番号　　［０００００１００７］

１．変更年月日　　１９９０年　８月３０日
［変更理由］　　新規登録
住　所　　東京都大田区下丸子３丁目３０番２号
氏　名　　キヤノン株式会社